Code: 23CC5O01   **R23**

SWARNANDHRA COLLEGE OF ENGINEERING & TECHNOLOGY
[AUTONOMOUS]
Seetharampuram, NARSAPUR-534 280
B. Tech V Semester Regular Examinations

CYBER SECURITY AND RISK MANAGEMENT

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

(CYBER SECURITY)

Note: 1. The question paper consists of two parts (**Part-A and Part-B**)
      2. Answer all questions from **Part-A**
      3. Answer all questions from **Part-B** with either or choice

Duration: 3 Hours   Max Marks: 70

PART-A (5x2=10M)

S No		Question	Cognitive Level	CO	Marks
1	a	Define "Information Security" and mention its main goal.	K1	1	2
	b	Write any two examples of secure communication methods.	K1	1	2
	c	What is meant by "Ethical Hacking"?	K1	2	2
	d	Expand XSS and explain it in brief.	K2	3	2
	e	What is "Risk Quantification" in cyber security?	K1	5	2

PART – B (5X12 = 60 M)

S. No		Question	Cognitive Level	CO	Marks
2	a	Explain the importance of protecting personal computers from cyber threats.	K2	1	6
	b	Describe the concept of "Safe Internet Usage" with examples.	K2	1	6
		OR			
3	a	Write about the basics of networking and its role in cyber security.	K2	1	6
	b	Explain secure communication protocols with suitable examples.	K3	1	6
4	a	Discuss the importance of privacy in cyber security with relevant examples.	K2	2	6
	b	Explain intellectual property rights in the context of cyber law.	K2	2	6
		OR			
5	a	Describe different types of cybercrimes with examples.	K1	2	6

	b	Write short notes on "Freedom of Speech" and "Fair Use" in digital space	K2	2	6
6	a	Explain the different stages of a penetration test.	K2	3	6
	b	Discuss the process of identifying and classifying web vulnerabilities.	K3	3	6
OR					
7	a	Explain common server and client types used in web architectures.	K2	3	6
	b	Write about defining a web application test process with examples.	K3	3	6
8	a	Describe password vulnerabilities and their prevention techniques.	K2	4	6
	b	Explain the concept of layered defense in network security.	K2	4	6
OR					
9	a	Discuss web server security issues and their mitigation.	K2	4	6
	b	Explain digital evidence collection and preservation in forensics.	K3	4	6
10	a	Describe the steps involved in business impact analysis.	K2	5	6
	b	Explain proactive and post-incident cyber services.	K3	5	6
OR					
11	a	Define business continuity and discuss its significance in cyber security.	K1	5	4
	b	Write about the phases of incident response with examples.	K2	5	8

Prepared by   **Verified by**   **Approved By**